To: U.S. Cybersecurity and Infrastructure Security Agency (CISA)
From: John Fouts
Subject: Urgent Firmware-Level Threat Submission – Evidence of Anomalous ELF Behavior in `csd-printer` Binary
Date: May 25, 2025

Summary of Submission:

This submission presents critical evidence obtained through **binary reverse engineering** of a suspicious ELF file named `csd-printer`, conducted using **Ghidra**. Screenshots enclosed in the attached ZIP archive expose function-level anomalies consistent with firmware-level compromise, malicious persistence, and impersonation of trusted Linux system services.

As a civilian without agency credentials, I have **not been granted full access to CISA's Malware Next Gen portal**, and received a denial message when attempting to upload through standard channels. Despite this, the threat is significant and demands urgent review by federal security personnel with relevant clearance.

Technical Highlights (See Screenshots):

- **Anomalous Entry Point (`entry`)**
    - Infinite loop (`while(true)`), no logic execution, obfuscation signature
    - See: `Screenshot from 2025-05-25 12-54-45.png`
- **Malicious D-Bus Registration and Impersonation**
    - `FUN_00102a90`, `FUN_00104a80`, and `FUN_00104bb0` bind to `.printer` and `settings-daemon` services
    - `g_dbus_own_name()` and `g_dbus_proxy_call_sync()` indicate service hijack
    - See: `Screenshots from 12:55:13`, `12:55:22`, and `12:56:07`
- **Use of Stack Canary Bypass & Obfuscation**
    - Multiple `__stack_chk_fail()` calls buried in unreachable branches
    - Common evasion technique and seen in `FUN_001049e0`, `00104a80`, `00104bb0`, `001035e0`
    - See: `Screenshots from 12:55:05`, `12:55:18`, `12:56:20`, `12:56:25`

- **Fake Printer Driver & Red Hat Configuration Injection**
  - Multiple hardcoded paths: `/com/redhat/PrinterDriversInstall`, `cinnamon-settings-daemon`
  - Function pointers suggest impersonation of Red Hat & Fedora trust anchors
  - See: `Screenshots from 12:55:22`, `12:56:38`, `12:56:29`
- **Empty and Decoy Functions**
  - Stubs with no logic (likely placeholders or obfuscation layers)
  - `FUN_00102fe0`, `FUN_00104930`, `FUN_00102f20`, etc.
  - See: `Screenshots from 12:55:47`, `12:55:31`, `12:56:57`

Evidence Archive:

Attached ZIP:
`2025-05-25-CISA-ghidra-csd-printer-binary-malware-screenshot-collection-functions-showing-anomalous-behavior-malicious-request-priority-review.zip`

Contains 18 high-resolution screenshots with full timestamps, each illustrating anomalous or malicious execution patterns observed in the disassembled binary.

Action Requested:

- Please **escalate to Malware Next Gen** or equivalent CISA division capable of evaluating UEFI/firmware-level compromise involving forged system services.
- Confirm **civilian submission receipt** for supplemental CISA case reference **#CCASE0092x**.
- Advise if sanitized submission is required via alternate channel.

This sample represents only **one component** of a broader, active firmware intrusion affecting health-critical infrastructure and devices. Further samples can be provided upon secure request.

Respectfully submitted,

John R. Fouts, MBA

icreateupwardspirals@gmail.com
JusticeForJohn